INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-11 18:19 UTC

Ransomware Attack on ChipSoft Disrupts Dutch and Belgian Healthcare EHR Services

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0166
Type	Threat Campaign
Severity	HIGH
Affected Products	ChipSoft HiX EHR platform, Dutch and Belgian hospitals
Discovery Source	Gemini

Executive Summary

A ransomware attack against ChipSoft, the Dutch vendor behind the HiX electronic health record platform, took the company's infrastructure offline and severed EHR access for hospitals across the Netherlands and Belgium. Affected facilities lost access to patient records and critical clinical workflows, forcing reversion to manual paper-based processes. This is a supply chain incident: a single vendor compromise simultaneously disrupted healthcare delivery at multiple hospital organizations, with no confirmed recovery timeline in public reporting as of discovery date.

Technical Analysis

ChipSoft's infrastructure hosting the HiX EHR platform was rendered unavailable following a ransomware deployment. No CVE has been assigned; this is an operational campaign rather than a discrete software vulnerability. MITRE ATT&CK techniques associated with this campaign include T1489 (Service Stop), T1486 (Data Encrypted for Impact), T1078 (Valid Accounts), T1657 (Financial Theft) and T1190 (Exploit Public-Facing Application). No specific threat actor group has been attributed in available public reporting. No patch is applicable; the incident is vendor-infrastructure-level. Affected hospitals lost access to HiX EHR services hosted or managed through ChipSoft's environment. No CVE, CVSS score, EPSS score, or CWE identifiers apply. IOCs have not been publicly disclosed by ChipSoft or attributed researchers as of the discovery date. Organizations dependent on ChipSoft-hosted or ChipSoft-managed HiX instances are affected; on-premises deployments with independent infrastructure may have different exposure depending on connectivity to ChipSoft systems. All sources are Tier 3; verify details against official vendor communications before operational decisions.

Action Checklist

1. Step 1: Containment. Identify which HiX services your organization consumes from ChipSoft (hosted, managed, or on-premises with ChipSoft connectivity). Isolate any active network connections to ChipSoft infrastructure until the vendor confirms systems are clean and restored. Contact your ChipSoft account representative immediately for current system status.
2. Step 2: Detection. Review network logs and firewall egress records for connections to ChipSoft-managed IP ranges and hostnames in the 72 hours preceding and following the incident discovery date (April 8, 2026, per published reporting). Confirm exact timing with your ChipSoft account representative. Check endpoint logs on clinical workstations for HiX client errors, unexpected session terminations, or authentication failures that may indicate service disruption or lateral movement. No specific IOCs are publicly available; monitor ChipSoft and threat intelligence feeds for disclosed indicators.
3. Step 3: Eradication. This is a vendor-side incident; eradication is ChipSoft's responsibility for hosted environments. For on-premises HiX deployments with ChipSoft administrative access or VPN connectivity, audit all active remote access sessions, disable non-essential ChipSoft remote access channels until the vendor provides written confirmation of remediation, and rotate credentials used by ChipSoft support accounts.
4. Step 4: Recovery. Do not reconnect to ChipSoft-hosted services until ChipSoft provides a signed incident report and confirmation of infrastructure integrity. When connectivity is restored, validate EHR data integrity by cross-referencing records entered during the outage period against paper backups. Monitor clinical workflows for missing or corrupted records from the disruption window.
5. Step 5: Post-Incident. Conduct a third-party dependency review: identify all critical clinical and operational systems that rely on a single external vendor for availability. Assess your downtime procedures: were paper-based fallback workflows documented and exercised before this incident? Update vendor risk assessments for healthcare IT suppliers to include ransomware scenario planning and contractual SLA obligations for breach notification and recovery timelines.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and your Data Protection Officer immediately if any ChipSoft-connected system processed or cached patient PHI/EHR data locally during the outage window, or if ChipSoft confirms ransomware actor access to data containing patient records, triggering GDPR Article 33 breach notification to the Dutch Autoriteit Persoonsgegevens within 72 hours and Belgian equivalents under applicable national law.
Recovery Notes	Do not restore HiX connectivity based solely on verbal confirmation from ChipSoft — require a written, signed infrastructure integrity attestation referencing specific remediation actions taken (ransomware removal, credential rotation, network re-segmentation). Upon reconnection, monitor HiX transaction logs and network egress to ChipSoft infrastructure continuously for a minimum of 30 days for anomalous data access patterns, bulk record queries, or unexpected outbound data volumes that could indicate a persistent threat actor retained in the ChipSoft environment. Reconcile all patient records created on paper during the outage against HiX data post-restoration, and retain paper originals for a minimum period consistent with Dutch healthcare records retention law (NEN 7510 and applicable WGBO obligations).

Forensic Artifacts	Firewall and proxy egress logs showing DNS queries and TCP session data to ChipSoft-managed IP ranges and hostnames (*.chipsoft.nl, HiX API endpoints) in the 72-hour window around 2026-04-08 — connection reset storms or timeout cascades pinpoint the exact propagation of the ransomware-induced outage to your network boundary. | Windows Application Event Log entries from clinical workstations running the HiX thick client, filtered for ChipSoft and HiX provider names, capturing server-unreachable errors and authentication token failures that timestamp your organization's loss of EHR access independent of ChipSoft's own incident timeline. | Active Directory Security Event Log entries (Event ID 4624, 4625, 4648, 4647) for all ChipSoft-provisioned support and service accounts, establishing whether any of these accounts were accessed during or after the ransomware event and from which source IPs — critical for determining whether attacker lateral movement extended beyond ChipSoft's own infrastructure. | VPN concentrator session logs for all ChipSoft remote access connections in the 30 days preceding the incident, including session durations, data volumes transferred, and source IP geolocation — anomalous off-hours or high-volume sessions may indicate pre-ransomware attacker use of compromised ChipSoft credentials. | Paper-based clinical records and handwritten logs created by hospital staff during the EHR downtime window — these are primary forensic evidence of the operational impact and serve as the authoritative data source for post-restoration EHR reconciliation and any regulatory impact assessment under GDPR or Dutch healthcare law.

Per-Action IR Details

Step 1: Containment — Identify which HiX services your organization consumes from ChipSoft (hosted, managed, or on-premises with ChipSoft connectivity). Isolate any active network connections to ChipSoft infrastructure until the vendor confirms systems are clean and restored. Contact your ChipSoft account representative immediately for current system status.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On the perimeter firewall or host firewall, create an explicit DENY rule targeting all ChipSoft-owned IP ranges and the HiX SaaS hostnames (e.g., *.chipsoft.nl, *.hix.nl — verify current ranges with your ChipSoft network documentation). On Windows endpoints, use: `netsh advfirewall firewall add rule name='BLOCK-ChipSoft' dir=out action=block remoteip=`. Use `netstat -an | findstr ESTABLISHED` on clinical workstations to identify any live sessions to ChipSoft endpoints before blocking. Document the block rule timestamp and retain as a containment action record.

Evidence: Before isolating: capture a full netstat dump from any workstation running the HiX client (`netstat -anob > netstat_pre_block__.txt`). Export current firewall connection state logs showing established sessions to ChipSoft IP ranges. If HiX uses a dedicated VPN tunnel (common for Dutch hospital deployments), capture VPN concentrator session logs showing ChipSoft support or management connections active at time of isolation. Preserve these before the block rule removes active session visibility.

Step 2: Detection — Review network logs and firewall egress records for connections to ChipSoft-managed IP ranges and hostnames in the 72 hours preceding and following the reported incident date (around 2026-04-08). Check endpoint logs on clinical workstations for HiX client errors, unexpected session terminations, or authentication failures that may indicate service disruption or lateral movement. No specific IOCs are publicly available; monitor ChipSoft and threat intelligence feeds for disclosed indicators.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Query firewall egress logs for all connections to ChipSoft IP ranges between 2026-04-05 and 2026-04-11 — look for unusual data volume spikes outbound (possible exfiltration staging) or repeated connection resets (service disruption onset). On Windows clinical workstations, query the Application Event Log for HiX client error events: `Get-WinEvent -LogName Application | Where-Object {$_.ProviderName -like '*HiX*' -or $_.ProviderName -like '*ChipSoft*'} | Select-Object TimeCreated, Id, Message | Export-Csv hix_events.csv`. Check Windows Security Event Log for Event ID 4625 (failed logon) and Event ID 4647 (user-initiated logoff) on workstations during the disruption window, which may indicate forced session termination caused by backend unavailability. Deploy Sysmon with a config that captures network connections (Event ID 3) to ChipSoft hostnames if not already present.

Evidence: Firewall/proxy logs showing DNS resolution attempts and TCP connections to ChipSoft-managed hostnames (*.chipsoft.nl, HiX API endpoints) in the 72-hour window around 2026-04-08 — unusual connection resets or timeout storms indicate the ransomware-induced outage propagating to your environment. Windows Application Event Log entries from the HiX thick client on clinical workstations showing server-unreachable or authentication-token-failure errors, which timestamp the exact moment your organization lost EHR access. Active Directory or LDAP authentication logs if HiX uses federated SSO — failed authentications sourced from ChipSoft-hosted identity services would appear here. Network flow data (NetFlow/IPFIX) showing volume anomalies to ChipSoft infrastructure in the days before the outage, which could indicate pre-ransomware reconnaissance or staging activity on ChipSoft's side visible from your egress.

Step 3: Eradication — This is a vendor-side incident; eradication is ChipSoft's responsibility for hosted environments. For on-premises HiX deployments with ChipSoft administrative access or VPN connectivity, audit all active remote access sessions, disable non-essential ChipSoft remote access channels until the vendor provides written confirmation of remediation, and rotate credentials used by ChipSoft support accounts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST IA-4 (Identifier Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export all Active Directory accounts or local accounts provisioned for ChipSoft support staff: `Get-ADUser -Filter {Description -like '*ChipSoft*' -or Description -like '*HiX*'} -Properties LastLogonDate, Enabled | Select-Object Name, SamAccountName, Enabled, LastLogonDate | Export-Csv chipsoft_accounts.csv`. Disable all such accounts immediately: `Disable-ADAccount -Identity `. For VPN access, pull the remote access VPN logs to identify all ChipSoft-sourced sessions in the past 30 days and terminate any active ones. If ChipSoft uses a jump host or PAM solution at your site, revoke its service account credentials and rotate the shared secrets. Document every account disabled and every credential rotated with timestamps for audit trail compliance.

Evidence: Before disabling ChipSoft support accounts, capture a last-logon and logon-history report for each account to establish whether any were used during or after the ransomware event — Active Directory Event ID 4624 (successful logon) and Event ID 4648 (logon with explicit credentials) filtered on ChipSoft account names. VPN concentrator logs showing source IPs, session durations, and volumes for all ChipSoft remote access sessions in the 30 days preceding the incident — anomalously long sessions or off-hours access may indicate attacker use of compromised ChipSoft credentials. If a PAM or privileged session management tool is in use, export session recordings or keystroke logs for any ChipSoft-initiated administrative sessions in the 72-hour pre-incident window.

Step 4: Recovery — Do not reconnect to ChipSoft-hosted services until ChipSoft provides a signed incident report and confirmation of infrastructure integrity. When connectivity is restored, validate EHR data integrity by cross-referencing records entered during the outage period against paper backups. Monitor clinical workflows for missing or corrupted records from the disruption window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Before reconnecting the HiX client to ChipSoft infrastructure, hash-verify any locally cached HiX application binaries or configuration files that may have been updated via ChipSoft's managed update mechanism during the incident window — use `Get-FileHash -Algorithm SHA256 ` and compare against pre-incident baseline hashes stored offline. Perform a structured reconciliation of paper-based records created during the outage: assign a clinical informatics resource to enter and date-stamp each paper record into HiX post-restoration, flagging the entry with an outage-period marker for audit traceability. Set up a temporary daily review for 30 days post-reconnection using HiX audit logs to detect any records with missing, truncated, or anomalous timestamps from the disruption window (2026-04-05 through full restoration date).

Evidence: ChipSoft's signed incident report and infrastructure integrity attestation — retain as a formal record per NIST IR-5 (Incident Monitoring) obligations. HiX application and database transaction logs from the moment of reconnection, capturing the first successful authentication and any data synchronization activity — these establish a clean reconnection baseline. Paper records created during the outage window, scanned and retained as source documents for any later audit of clinical data continuity. Network connection logs from the first 24 hours post-reconnection showing only expected ChipSoft endpoints communicating, confirming no unexpected lateral infrastructure is being accessed.

Step 5: Post-Incident — Conduct a third-party dependency review: identify all critical clinical and operational systems that rely on a single external vendor for availability. Assess your downtime procedures: were paper-based fallback workflows documented and exercised before this incident? Update vendor risk assessments for healthcare IT suppliers to include ransomware scenario planning and contractual SLA obligations for breach notification and recovery timelines.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Build a vendor dependency map using a simple spreadsheet: for each clinical system (EHR, PACS, pharmacy, lab), document vendor name, hosting model (SaaS/managed/on-prem), remote access method, last vendor risk assessment date, and contractual breach notification SLA. Flag any single-vendor dependencies with no documented downtime procedure. Schedule a tabletop exercise specifically modeled on the ChipSoft HiX outage scenario — simulate 72-hour EHR unavailability and walk clinical and IT staff through the paper-based fallback procedure to identify gaps. Review contracts with ChipSoft and equivalent vendors for Article 28 GDPR processor obligations and NEN 7510 (Dutch healthcare information security standard) compliance requirements, which are directly applicable to Dutch hospital operators in this incident.

Evidence: Lessons-learned documentation from this incident capturing: exact duration of HiX unavailability per affected department, volume of paper records created, staff hours expended on manual processes, and any patient safety near-misses attributable to EHR inaccessibility — this constitutes the risk quantification input for vendor risk reassessment. Current vendor contracts with ChipSoft reviewed for breach notification timelines, RTO/RPO commitments, and indemnification clauses — absence of these provisions is a finding. Existing business continuity and downtime procedure documentation (or confirmed absence thereof), retained as evidence for the post-incident improvement action plan.

Detection Guidance

No confirmed IOCs (IPs, domains, file hashes, or URLs) have been publicly released as of the discovery date. Detection efforts should focus on behavioral and availability signals. Review network flow data for unexpected drops in connectivity to ChipSoft infrastructure around April 8, 2026. Check SIEM for authentication anomalies against HiX endpoints: credential stuffing patterns, use of service accounts outside expected hours, or bulk authentication failures aligning with T1078 (Valid Accounts). For on-premises HiX deployments, monitor Windows Event Logs for service stop events (Event ID 7036) on HiX-related services and for volume shadow

copy deletion commands (Event ID 4688 with vssadmin or wmic as process name), consistent with T1489 and T1486 pre-encryption activity. Absent disclosed IOCs, priority detection is availability monitoring of ChipSoft-dependent services and immediate escalation on any anomalous lateral movement from systems with ChipSoft remote access credentials. Update threat intelligence platforms with ChipSoft as a tracked vendor for this campaign when IOCs are published.

Framework Mappings

MITRE-ATTACK

- **T1489** — Service Stop
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1657** — Financial Theft
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

- **A.5.21** — Managing information security in the ICT supply chain

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1489	Service Stop	Impact
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Dutch healthcare software vendor goes dark after ransomware attack	https://www.theregister.com/2026/04/08/chipsoft_ransomware/	T3
Healthcare IT solutions provider ChipSoft hit by ransomware attack	https://www.bleepingcomputer.com/news/security/healthcare-it-soluti...	T3
Healthcare software company ChipSoft hit by ransomware attack	https://www.paubox.com/blog/healthcare-software-company-chipsoft-hi...	T3
Ransomware attack on ChipSoft knocks EHR services offline across ...	https://securityaffairs.com/190615/cyber-crime/ransomware-attack-on...	T3
Ransomware knocks Dutch healthcare software vendor offline - Reddit	https://www.reddit.com/r/cybersecurity/comments/1shx5iq/ransomware_...	T3

Generated 2026-04-11 18:19 UTC by TJS Security Command Center